

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
SOUTHERN DIVISION

Case No. 7:20-cr-00167-M-3

UNITED STATES OF AMERICA,

Plaintiff,

v.

JORDAN DUNCAN,

Defendant.

ORDER

This matter comes before the court on the Defendant Jordan Duncan's ("Duncan") motion to suppress [DE 341]. For the following reasons, the court denies the motion.

I. Background

A. Factual Background

In November 2019, law enforcement began investigating a white supremacist group for suspected firearms trafficking. In support of a search warrant application submitted to a magistrate judge in this district, the applying officer attached an affidavit providing extensive details regarding the group's firearm trafficking activity. *See* DE 342 at 10.

The affidavit stated that Liam Collins would discuss manufacturing and selling unserialized guns and silencers with others via encrypted messaging applications (e.g., Wire) and that he would accept payment for those firearms and parts using Venmo. He would also send videos and pictures of illegally manufactured firearms and silencers in response to inquiries from potential buyers. Collins commissioned Paul Kryscuk, a contact in his iCloud account, to manufacture and ship the firearms and parts. Together, they distributed deconstructed firearms packages to their coconspirators, namely Duncan, Joseph Maurino ("Maurino"), and Justin

Hermanson, as well as other active duty servicemembers at Camp Lejeune and elsewhere. With respect to one of these transactions involving a cooperating witness, Collins attempted to use FaceTime to communicate with said cooperating witness. In July 2020, Maurino, Duncan, and another individual closely associated with Collins met in Boise, Idaho to participate in firearms training. *See generally* DE 342 at 13–23.

On August 27, 2020, the magistrate judge issued the requested warrant to search Duncan’s and other group members’ iCloud accounts (the “iCloud Warrant”). With respect to Duncan, the Warrant required Apple to disclose extensive categories of information contained in Duncan’s iCloud account, including all emails and instant messages from May 11, 2018 to August 27, 2020 as well as “all files and other records” stored on the account. *See* DE 342 at 4–6. The Warrant also authorized the government to review that data to retrieve evidence of violations of 18 U.S.C. § 922(a)(5) (transfer of firearms to nonresidents) and 26 U.S.C. § 5801-72 (violations of the National Firearms Act). *See id.* at 7–8.

Law enforcement applied for another warrant (the “Device Warrant”), which was later issued on October 16, 2020, to search Duncan’s computers, cellular phones, and other electronic storage devices seized from his residence, vehicle, or person for information relating to violations of 18 U.S.C. § 922(a)(1)(A) (unlicensed dealing in firearms), 18 U.S.C. § 922(a)(5) (transfer of firearms to nonresidents), 26 U.S.C. § 5801-72 (violations of the National Firearms Act), 18 U.S.C. § 641 (theft of government property), and 18 U.S.C. § 371 (conspiracy to commit the suspected violations). *See* DE 343 at 39–46. The affidavit supporting this Warrant provided the same factual basis supporting the iCloud Warrant. It further provided that Duncan moved to Boise, Idaho on September 8, 2020, and that Collins later lived at the same residence as Duncan. Additionally, during their firearms training sessions, the group members would collect video

footage that they would then upload to their iCloud accounts and compile into group promotional materials displaying neo-Nazi symbols and sentiments. DE 343 at 2–13.

A third warrant (the “Supplemental Warrant”) was issued on February 2, 2021. This Warrant authorized law enforcement to search Duncan’s iCloud account and previously seized electronic storage devices for information evidencing violations of 18 U.S.C. § 641 (conversion of public records) and 18 U.S.C. § 793, specifically subsections (e) (gathering and transmitting defense information) and (g) (conspiracy to commit listed offense). *See* DE 344 at 53–59. The affidavit in support of the Warrant provides extensive details regarding Duncan’s retention and distribution of national defense and other public documents. *See generally* DE 344 at 16–36.

B. Procedural Background

On August 18, 2021, the United States charged Duncan with conspiracy to manufacture and ship firearms in violation of 18 U.S.C. § 922(a)(1)(A) (Count One, 18 U.S.C. § 371) and conspiracy to destroy an energy facility (Count Five, 18 U.S.C. § 1366(a)). DE 149. On October 2, 2023, Duncan filed the instant motion to suppress electronic evidence searched and seized from his iCloud account and electronic storage devices. DE 341. The United States timely responded. The court is fully apprised.

II. Discussion

The Fourth Amendment provides the right of the people “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” *See* U.S. Const. amend. IV. The Supreme Court has “repeatedly affirmed” that “the ultimate touchstone of the Fourth Amendment is reasonableness.” *Heien v. North Carolina*, 574 U.S. 54, 60-61 (2014).

Duncan argues that the court should suppress the evidence resulting from the searches of his iCloud account, iPhone, and other electronic storage devices because the iCloud, Devices, and Supplemental Warrants failed to satisfy the particularity requirement of the Fourth Amendment. *See* DE 341. According to Duncan, the Warrants allowed law enforcement to conduct an evidentiary search whose scope far exceeded the probable cause described in their supporting affidavits. *See* DE 341 at 7–9. Duncan argues that law enforcement should have placed limits on their searches based on the subject and time of the electronic information. *See id.* at 9–12. Because they failed to do so, each warrant in his view authorized a “general, exploratory rummaging” through his electronic information. *See* DE 341 at 8–9 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

The Fourth Amendment requires sufficient particularity when issuing warrants. U.S. Const. amend. IV. “[A] warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize.” *United States v. Blakeney*, 949 F.3d 851, 863 (4th Cir. 2020). “By limiting the authorization to search to the specific areas and things for which there is probable cause to search,” the Fourth Amendment “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Failure to reasonably limit the scope of the authorized search to the specific areas and things for which probable cause exists amounts to impermissible overbreadth. *See, e.g., United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006); *United States v. Manafort*, 323 F. Supp. 3d 795, 801 (E.D. Va. 2018).

Here, the Warrants described the specific places to be searched and items to be seized. The iCloud Warrant required Apple to disclose ten, albeit expansive, categories of information¹ to law enforcement. *See* DE 342 at 4–6. This Warrant also specified that law enforcement would review and seize any evidence of suspected firearm trafficking involving the account since June 7, 2016. *Id.* The Devices Warrant specifically authorized the search to cover any “[c]omputers, cellular phones, and electronic storage devices, emails, papers, tickets, notes, receipts, and other items relating to [the] purchase, manufacture, distribution, sale, or transfer of firearms or NFA weapons” seized from his residence, vehicle, or person. DE 343 at 42. And the Supplemental Warrant specifically confined the search by listing the iCloud account and previously seized electronic storage devices as the places to be searched for evidence relating to the conversion of public documents. DE 344 at 53–55. The executing officer for each Warrant knew “precisely what he has been authorized to search for and seize.” *Blakeney*, 949 F.3d at 863.

Duncan does not dispute that probable cause supported the authorizations as to the aforementioned places to be searched and things to be seized. Indeed, Duncan concedes that law enforcement provided probable cause to believe his iCloud account would contain images and videos of training sessions implicating his association with individuals trafficking firearms without a federal license. *See* DE 341 at 8. He also concedes that law enforcement reasonably believed that a search of the iCloud account would uncover transaction records and associated media resulting from past sales of illegally manufactured firearms and firearm parts. *See id.* The record supports these concessions. *See* DE 342 at 23, 25. Since probable cause existed to search “the specific areas

¹ The iCloud Warrant specifically commanded Apple to disclose the account’s identification; devices; emails and instant messages between May 11, 2018 to August 27, 2020; activity, connection, and transactional logs; geographic locations; service provider records; communications with Apple; and decryption. DE 342 at 4–6.

and things” listed in the Warrants for evidence of the specified offenses, the Warrants were not impermissibly overbroad. *See Garrison*, 480 U.S. at 84; *Manafort*, 323 F. Supp. 3d at 801.

The court recognizes that Duncan’s argument does not turn on whether probable cause existed, but rather to what extent. In particular, he contends that probable cause did not extend to *all* the information contained in his iCloud account or electronic storage devices. *See* DE 341 at 8. However, probable cause to search his devices for evidence of the listed offenses properly extended to searching the entirety of those devices for evidence of those offenses. *See United States v. Cobb*, 970 F.3d 319, 329 (4th Cir. 2020). Despite the “sheer amount of information contained” in those devices, searching each one was analogous to searching “a file cabinet containing a large number of documents.” *United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010). As long as officers provide probable cause to search those devices, they “are generally not required to predict the items of evidence that an electronic search will uncover or predict where on the computer [or other storage device] the evidence will be found.” *United States v. Bolling*, 2023 WL 5616188, at *6 (S.D.W. Va. Aug. 30, 2023) (citing *Cobb*, 970 F.3d at 329). This principle is especially true in this case because law enforcement knew that Duncan and his coconspirators regularly used encrypted messaging applications, fake driver’s licenses, aliases, and deconstructed firearm shipments to avoid detection. *See, e.g.*, DE 342 at 14, 17–18, 22. Given the realities of the investigation, “more specificity was not required under the Fourth Amendment, nor was limiting the scope of the computer search practical or prudent.” *See Cobb*, 970 F.3d at 329.

Duncan has not presented any reason why this court should treat cloud accounts differently from computers or other electronic storage devices when determining the extent to which probable cause exists to search all of the information contained therein. After all, iCloud accounts serve as another way for Apple device users to store local device files and data. DE 342 at 27. Although

the information on an iCloud account can often differ quantitatively and qualitatively from its local storage counterpart, for example by often storing information pertaining to various local storage devices associated with a single Apple User ID, “neither the quantity of information, nor the form in which it is stored, is legally relevant” for particularity requirement purposes. *See Williams*, 592 F.3d at 524 (quoting *United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008)); *Cobb*, 970 F.3d at 329 (reiterating that “so long as the Fourth Amendment’s basic requirements of probable cause and particularity are met, the executing officers are impliedly authorized to open each file on a computer and view its contents, at least cursorily” (cleaned up)).

In the alternative, even if the Warrants violated the particularity requirement, the good faith exception to the exclusionary rule nonetheless applies. “[E]vidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant” should generally not be excluded. *United States v. Leon*, 468 U.S. 897, 922 (1984). However, if the warrant was “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers [could not have] reasonably presume[d] it to be valid,” exclusion may be justified. *Id.* at 923.

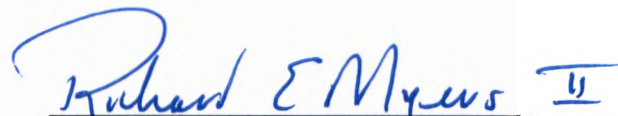
It is possible to argue that the Warrants here may have failed to sufficiently particularize the place to be searched or the things to be seized, but “whether they did is not an open and shut matter; it is a close enough question that the warrants were not ‘so facially deficient’ that the [law enforcement] agents who executed them could not have reasonably believed them to be valid.” *United States v. Blake*, 868 F.3d 960, 975 (11th Cir. 2017); *see also United States v. McCall*, 84 F.4th 1317, 1328 (11th Cir. 2023); *United States v. Cawthorn*, 2023 WL 5163359, at *4 (D. Md. July 13, 2023); *United States v. Ray*, 541 F. Supp. 3d 355, 401–02 (S.D.N.Y. 2021); *United States v. Chavez*, 423 F. Supp. 3d 194, 208 (W.D.N.C. 2019). With respect to the application of the good

faith exception, Duncan offers no reason for this court to disagree with the weight of relevant authority.

III. Conclusion

For the foregoing reasons, Duncan's motion to suppress [DE 341] is DENIED.

SO ORDERED this 22^d day of January, 2024.



RICHARD E. MYERS II
CHIEF UNITED STATES DISTRICT JUDGE